REMARKS

Claims 1-78 are pending in the present application. Claims 1 and 29 have been amended herewith. Reconsideration of the claims is respectfully requested.

I. General Administration Matters

Applicants wish to point out several matters pertaining to the 07/21/2003 Office Action (paper #4) that prohibited Applicants from fully responding to the rejection of Claims 1-78 (such claims being indicated as being rejected on the Office Action Summary page):

(1) No reason was given, either statutorily or in the comments section, for the rejection of Claims 47 and 73.

(2) In the Detailed Action, in the 35 U.S.C. 102(b) rejection, the following claims were listed as being rejected under 35 U.S.C. 102(b) : Claims 1, 3-5, 9, 13-15, 18-20, 22, 24, 26-29, 31-33, 37, 41-43, 46, 48, 50, 52, 54-55, 62, 71, 77-74, 77-76, 77-78. Further clarification is requested regarding what is meant by Claims 77-74 and 77-76.

(3) Claim 19 is listed as part of the claims subject to the 35 U.S.C. 102(b) rejection, yet Claim 19 is not mentioned in the remarks section of the 35 U.S.C. 102(b) rejection. Somewhat related, Claim 19 is also listed as part of the claims subject to the 35 U.S.C. 103 rejection, and Claim 19 is mentioned in the remarks section of the 35 U.S.C. 103 rejection. Further clarification is requested regarding the statutory basis for the rejection of Claim 19.

(4) Claims 56, 57, 64, 65, 66 and 75 are mentioned in the remarks section of the 35 U.S.C. 102(b) rejection, but are not included in the list of claims being rejected under 35 U.S.C. 102(b). Further clarification is requested regarding the statutory basis for the rejection of Claims 56, 57, 64, 65, 66 and 75.

(5) The 35 U.S.C. 103 rejection of Claims 23 and 51 identifies Thompson, Jr. et al. U.S. Patent 5978483 as being used in rejecting such claims, and yet this reference is not listed on the Notice of References Cited on PTO-Form 892. Applicants request issuance of a new PTO Form 892 indicating this reference has been formally considered and made of record by the Examiner.

II. **35 U.S.C. § 102, Anticipation**

The Examiner rejected Claims 1, 3-5, 9, 13-15, 18-20, 22, 24, 26-29, 31-33, 37, 41-43, 46, 48, 50, 52, 54-55, 62, 71, 77-74, 77-76, 77-78 under 35 U.S.C. § 102 as being anticipated by Brinkmeyer et al. U.S. Patent 5838251. Subject to not being able to fully respond to this rejection as described above, this rejection is respectfully traversed.

Generally speaking, the claimed invention is directed to a method and system that eliminates the requirement for a physical key that is used to operate a lock, whereas the cited reference is specifically directed to a technique for programming a physical key used to operate a lock. As discussed in the Description of Related Art on page 1 of Applicants' patent application, known locking systems typically include a mechanical lock requiring a physical key or keycard that is inserted into the lock in order to open the lock for access to the contents of the locked object, and that these physical keys and keycards are inconvenient since they are prone to being misplaced, etc. The present invention overcomes these drawbacks by using an electronic key in lieu of such physical key or keycard (Specification page 2, lines 16-30; page 3, lines 5-7). This is in contrast to the teachings of the cited reference, which specifically teaches a technique for programming a physical key (Brinkmeyer Col. 1, lines8-20; Col. 2, lines 31-35; Col. 4, lines 21-30; Col. 6, lines 5-14 and 39-44; Figure 1, element 4, etc.). Thus, the techniques described by Brinkmeyer are fundamentally different from Applicants' invention, and in fact expressly teach away from a method and system of using electronic keys in place of physical keys.

Another fundamental difference between Applicants claimed invention and the teachings of the cited Brinkmeyer reference pertains to the how the electronic key is managed, and in particular to the use of the secondary key code cited in independent Claims 1, 29, 76-78. This secondary key code is generated from, or generated based on, a master key code and is then subsequently used by a wireless communication device to operate the electronic locking device (Claims 1 and 29), or is received and used in authenticating another received key code to determine whether to operate the electronic locking device (Claims 76-78). The Examiner states that Brinkmeyer's decoding of the encoded key reads on this secondary key code. However, the expressed purpose of Brinkmeyer is to decode the encoded key in the vehicle component itself (the example

given being a vehicle key) so that unencoded data is never exposed outside the component itself in order to reduce exposure to unauthorized access of the unencoded data (Brinkmeyer Col. 1, lines 56-67; Col. 3, lines 18-23). Thus, Brinkmeyer expressly abhors any transmitting or receiving of such an unencoded key and therefore Brinkmeyer's unencoded key does not read on the claimed secondary key code.

Specifically with respect to Claim 1 (and dependent claims thereof), such claim recites "transmitting the secondary key code to the wireless communication device, wherein the secondary key code is used by the wireless communication device to operate the electronic locking device in lieu of by a tangible device". As can be seen, this claimed feature recites (i) a secondary key code that is used by a wireless communication device to operate the electronic locking device, and this is done instead of by use of a tangible device to operate the locking device; and (ii) the secondary key code is transmitted to the wireless device. The cited Brinkmeyer reference uses a tangible vehicle key (Figure 1, element 4; Col. 1, lines 8-20), and thus does not teach or suggest the claimed feature of "wherein the secondary key code is used by the wireless communication device to operate the electronic locking device in lieu of by a tangible device". In addition, the cited reference does not teach the claimed secondary key code. The Examiner equates Brinkmeyer's decoding of encoded data as reading on this secondary key code. Applicants show that this cannot be the case, as the claim recites "transmitting the secondary key code to the wireless device". The teachings of Brinkmeyer are expressly directed to techniques such that *unencoded data is never transmitted*, and thus Brinkmeyer's unencoded data does not equate with the claimed secondary key code, because Claim 1 recites that the secondary key code is transmitted to a wireless device. See, for example, Brinkmeyer's discussion at Col. 3, lines 18-23, where it states:

> "The risk of an unauthorized person acquiring the data information to be transmittede from the central office and stored in the individual vehicle components to be programmed is minimized by virtue of the fact that the data to be transmitted are *decoded only in the vehicle component to be programmed* with these data". (emphasis added by Applicant)

Thus, Brinkmeyer expressly teaches away from transmitting unencoded data, and therefore Brinkmeyer's unencoded data does not read on the claimed feature of "transmitting the secondary key code to the wireless device".

Claim 1 (and dependent claims thereof) is thus shown to not be anticipated by the cited reference.

Further with respect to Claim 5 (and Claim 33), Applicants show that such claim recites "transmitting the secondary key code to the electronic locking device using at least one of a wired communication link and wireless communication link". This is in addition to the transmitting step of Claim 1 (of which Claim 5 depends upon), which recites "transmitting the secondary key code to the wireless communication device". Thus, Claim 5 recites transmitting the secondary key code to both the wireless communication device *and* the electronic locking device. The Examiner equates this claimed secondary key code to Brinkmeyer's unencoded data. Applicants show that Brinkmeyer does not teach transmitting of such unencoded data to *both* a wireless communication device *and* an electronic locking device. The features of Claim 5 advantageously allow for an improved method of using an electronic key to operate an electronic locking device, in that the electronic key (the secondary key code) is transmitted to both the wireless communication device and the electronic locking device to enable subsequent use of the electronic key by the wireless device when attempting to access the electronic locking device (Specification page 11, lines 2-16).

Further with respect to Claim 14 (and Claim 42), Applicants show that the cited reference does not teach the claimed feature of "wherein transmitting the secondary key code to the electronic locking device is performed at a remote time from transmitting the secondary key code to the wireless communication device". The Examiner cites Brinkmeyer Col. 6, lines 45-56 as reading on this claimed feature. Applicants show that, to the contrary, this passage states that *encoded data* is transmitted over telephone link (10) to service center (1). In rejecting Claim 1, the Examiner equated this encoded data as reading on the claimed 'master key code', so it is not seen how transmitting this alleged 'master key code' reads on the claimed feature of "transmitting the *secondary key code*". The claimed master key code and secondary key code are different codes, and a teaching of transmitting of one (Brinkmeyer's encoded data which is alleged to be the

claimed master key code) reads on transmitting of the other (the secondary key code). Thus, Claim 14 (and Claim 42) is further shown to not be anticipated by the cited reference.

Further with respect to Claim 15 (and Claim 43), Applicants show that the cited reference does not teach the claimed steps of "receiving a key code from the wireless communication device" and "authenticating the key code based on the secondary key code". The Examiner cites Brinkmeyer Col. 6, lines 65-67 as teaching authenticating the key code and transmitting a command to operate the electronic locking device of the key code is authenticate. Notably absent is any assertion of the claimed step of "receiving a key code from the wireless communication device", where this received key code is the key code being authenticated. This is because there is no such teaching. Claim 15 introduces yet another key code (the key code), which is in addition to the master key code and the secondary key code. The Examiner apparently makes no assertion as to any teaching of this third key code (the key code) because there is no such teaching of a third key code. Therefore, Claim 15 (and Claimj 43) is further shown to not be anticipated by the cited reference.

Further with respect to Claim 22 (and Claim 50), Applicants show that the cited reference does not teach the claimed step of "maintaining a record of secondary key codes used to access the electronic locking device", which advantageously allows for a passive electronic locking device where authentication is performed elsewhere (i.e. not by the electronic locking device itself), where the record of secondary key codes (i.e. a plurality of secondary key codes) are maintained (Specification page 17, lines 9-32). The Examiner cites Col. 45-49 of Brinkmeyer as teaching this claimed feature. Applicants show that Brinkmeyer does not have a Col. 45-49, and thus Brinkmeyer Col. 45-49 does not teach this claimed feature, as alleged. Claim 22 (and Claim 50) is thus shown to not be anticipated by the cited reference.

Further with respect to Claim 24 (and Claim 52), Applicants show that the cited reference does not teach the claimed feature of "wherein authenticating the key code based on the secondary key code includes determining an activation/expiration time of the secondary key code and determining if a current time is within the activation/expiration time". In rejecting Claim 24, the Examiner cites Brinkmeyer Col.

11, lines 37-50 as teaching this claimed feature. Applicants show that there, Brinkmeyer states:

> "Then, by means of the devices shown in FIGS. 1 and 2 and with the described procedure, on a protected path, usage authorization data for an individual vehicle desired by a customer can be transmitted to this customer from central office (20), specifically to his key (4). These can be usage authorization data which allow the customer only limited mobility with the desired vehicle. This mobility limitation can be accomplished for example by virtue of the fact that the usage authorization data transmitted by central office (20) are selected so that key (4) can unlock or turn off the anti-theft protection system of the vehicle only for a certain number of actuations, such as engine starts, for example."

As can be seen, this passage discusses the ability to limit mobility of a vehicle by allowing the key (4) to unlock or turn off the anti-theft protection system only for a certain number of actuations. A teaching of programming data in a key to limit physical mobility of a vehicle does not teach the claimed feature of "wherein *authenticating the key code* based on the secondary key code *includes* determining an activation/expiration time of the secondary key code and determining if a current time is within the activation/expiration time". While Brinkmeyer does go on to state at Col. 11, lines 51-58 that it is possible to limit mobility in terms of time, this is accomplished by presetting individual values by a central office, which are then transmitted and programmed into the key (4), and upon its first operation of the vehicle, to components on the vehicle. Thus, Brinkmeyer merely states that limiting values required for time limitations are transmitted "to components on the vehicle" (Col. 11, lines 55-58). There is no teaching of the claimed determination of the activation/expiration as being a part of the key code authentication itself, as claimed. Thus, Claim 24 (and Claim 52) is shown to not be anticipated by the cited reference.

With respect to Claim 26 (and Claim 54), such claim recites a polling of the electronic locking device itself. The Examiner cites Brinkmeyer Col. 10, lines 47-47 as

teaching this claimed feature. Applicants show that this discussion is with respect to Brinkmeyer's key, and makes no mention of polling the electronic locking device (which is different than the key). For example, the passage beginning at Col. 10, line 47 states:

> "Another possible application of the device if FIG. 2 relates to the possibility of status inquiries via central office (20)."

A review of Brinkmeyer's FIG. 2 shows a remote central office (20) and individual center (1) having a program device (3) used to program the components (33, 35 and 38). There are no electronic locking devices shown in Figure 2, nor is there any data path from the vehicle to the central office that would allow lock status to flow, and so the teachings of any type of status inquiry regarding FIG. 2 is shown to not include a teaching of polling the electronic locking devices themselves, as claimed. Thus, the cited passage does not teach polling of the electronic locking device, as claimed, and therefore Claim 26 (and Claim 54) is not anticipated by the cited reference.

Further with respect to Claim 27 (and Claim 55), such claim recites specifics of the status information received from the electronic locking device in response to polling the electronic locking device. For similar reasons to those given above regarding Claim 26, as there is no teaching of polling the electronic locking device, there similarly is no received status from the electronic locking device in response to such (non-existent) polling of the electronic locking device. Thus, Claim 27 (and Claim 55) is not anticipated by the cited reference, as there is at least one missing claimed element.

With respect to Claim 29 (and dependent claims thereof), Applicants traverse the rejection of such claims for similar reasons to those given above regarding Claim 1.

With respect to Claim 76, such claim recites "receiving, from a key supplier, a secondary key code". In rejecting Claim 76, the Examiner states that Brinkmeyer teaches

> "receiving a *master key code* (encoded data) from a master key supplier (20) and generating a secondary key code from the master key code and transmitting the secondary key code to the wireless communication device of the vehicle".

Therefore, even assuming arguendo that the Examiner's statement is true, it does not establish a teaching of "receiving, from a key supplier, a *secondary key code*", as is claimed in Claim 76. Therefore, Claim 76 is not anticipated by the cited reference as there are missing claimed elements not taught by the cited reference.

With respect to Claims 77 and 78, Applicants traverse the rejection of such claims for similar reasons to those given above regarding Claim 76.

III. 35 U.S.C. § 103, Obviousness

(A) The Examiner rejected Claims 2, 19, 21, 30, 46, 49, 58, 63, 67 and 72 under 35 U.S.C. § 103 as being unpatentable over Brinkmeyer et al. U.S. Patent 5838251 in view of Hyatt, Jr. et al. U.S. Patent 5745044. This rejection is respectfully traversed.

Applicants initially traverse the rejection of these claims for reasons given above regarding the teaching deficiencies of Brinkmeyer with respect to the independent and dependent claims that these claims depend upon.

Further with respect to Claim 2 (and Claim 58), the Examiner states that Brinkmeyer teaches a secondary key code that includes a secondary key code portion at Col. 7, lines 24-25. Applicants show error, as this passage discusses use of secret coding value that is used to encode the data sent from the central office. The Examiner has already equated the secondary key code to the unencoded data, so it is not seen how a secret code used to *encode* data is somehow a part of the *unencoded* data.

The Examiner goes on to state that Brinkmeyer teaches at Col. 11, line 35 the claimed secondary key code having an identification portion. Applicants show error, in that this passage states that the physical, tangible key has an identification number. Applicants claimed identification is with respect to the secondary key *code*, and not with respect to a tangible key. Thus, Claim 2 (and Claim 58) is further shown to have claimed elements not taught or suggested by the cited references.

(B) The Examiner rejected Claims 6-7 and 34-35 under 35 U.S.C. § 103 as being unpatentable over Brinkmeyer et al. U.S. Patent 5838251 in view of Gonzales et al. U.S. Patent 5936544. This rejection is respectfully traversed.

Applicants initially traverse the rejection of these claims for reasons given above regarding the teaching deficiencies of Brinkmeyer with respect to the independent and dependent claims that these claims depend upon.

Further with respect to Claims 6 (and Claim 34) and Claim 7 (and Claim 35), none of the cited references teach or suggest the claimed feature of "wherein transmitting the secondary key code to the electronic locking device includes transmitting the secondary key code based on a network address of the electronic locking device" (Claim 6) or "wherein transmitting the secondary key code to the electronic locking device includes broadcasting the secondary key code along with an identifier of the electronic locking device" (Claim 7). The Examiner concedes that Brinkmeyer is silent on teaching this, but then states that Gonzales teaches this at Col. 5, lines 2-8. Applicants show that this cited passage teaches keeping track of time and date by counting clock inputs of an oscillator, and writing data into an EEPROM through an electronic switch while increasing and decreasing the amount of power consumed by a load. It has nothing to do with transmitting the secondary key code *based on a network address of the electronic locking device* (Claims 6 and Claim 34) or broadcasting the secondary key code *along with* an identifier of the electronic locking device (Claims 7 and 35). Therefore, Claims 6-7 and 34-35 are further shown to have claimed elements not taught or suggested by the cited references.

(C) The Examiner rejected Claims 8, 36, 59 and 68 under 35 U.S.C. § 103 as being unpatentable over Brinkmeyer et al. U.S. Patent 5838251 in view of Larson U.S. Patent 5815557. This rejection is respectfully traversed.

Applicants traverse the rejection of these claims for reasons given above regarding the teaching deficiencies of Brinkmeyer with respect to the independent and dependent claims that these claims depend upon.

(D) The Examiner rejected Claims 10-11, 25, 38-39, 53, 60-61, 69 and 70 under 35 U.S.C. § 103 as being unpatentable over Brinkmeyer et al. U.S. Patent 5838251 in view of Kucharczyk et al. U.S. Patent 6570488. This rejection is respectfully traversed.

Applicants traverse the rejection of these claims for reasons given above regarding the teaching deficiencies of Brinkmeyer with respect to the independent and dependent claims that these claims depend upon.

(E) The Examiner rejected Claims 12 and 40 under 35 U.S.C. § 103 as being unpatentable over Brinkmeyer et al. U.S. Patent 5838251 in view of Henderson et al. U.S. Patent 4947163. This rejection is respectfully traversed.

Applicants initially traverse the rejection of these claims for reasons given above regarding the teaching deficiencies of Brinkmeyer with respect to the independent and dependent claims that these claims depend upon.

Applicants further traverse the rejection of Claim 12 (and Claim 40) by showing that contrary to the Examiner's assertion that Brinkmeyer teaches programming of a locking device, Brinkmeyer teaches programming of a key (Col. 4, lines 19-20). While the key may be used with a locking device, Brinkmeyer certainly does not teach programming or reprogramming of an electronic locking device itself.

Nor does the cited Henderson reference overcome this deficiency. Specifically, there is no confirmation message that confirms reprogramming of the electronic locking device to accept the secondary key code. Therefore, Claims 12 and 40 are further shown to not be obvious in view of the cited references.

(F) The Examiner rejected Claims 16-17 and 44-45 under 35 U.S.C. § 103 as being unpatentable over Brinkmeyer et al. U.S. Patent 5838251 in view of Henry et al. U.S. Patent 5774059. This rejection is respectfully traversed.

Applicants traverse the rejection of these claims for reasons given above regarding the teaching deficiencies of Brinkmeyer with respect to the independent and dependent claims that these claims depend upon.

(G) The Examiner rejected Claims 23 and 51 under 35 U.S.C. § 103 as being unpatentable over Brinkmeyer et al. U.S. Patent 5838251 in view of Thompson et al. U.S. Patent 5978483. This rejection is respectfully traversed.

Applicants traverse the rejection of these claims for reasons given above regarding the teaching deficiencies of Brinkmeyer with respect to the independent and dependent claims that these claims depend upon.

IV. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: October 21, 2003

Respectfully submitted,

Stephen J. Walder, Jr.
Reg. No. 41,534

Wayne P. Bailey
Reg. No. 34,289
Carstens, Yee & Cahoon, LLP
P.O. Box 802334
Dallas, TX 75380
(972) 367-2001
Attorneys for Applicants